Minnesota Lawyer

Breaking Ethics Issues – Benchslaps and Cyber Threats

By: Charles Lundberg May 12, 2016

Over the last few weeks, the legal press has been buzzing with a number of breaking topics about ethics and the law of lawyering. Here are two[1]:

Benchslaps – The Judge as Bully?

Everyone knows what a Benchslap is, right?

For the unfamiliar, benchslap originally referred to one judge snarking at another, but now refers to any time a member of the bench crushes an attorney with wit, rage, or both. We all live in terror of it happening to us, but we circulate every benchslap that comes our way. Benchslaps are one-half "thank god I've dodged that bullet thus far," one-half gallows humor, and one-half schadenfreude. Yeah, that is three halves.[2]

The term has been defined in *Black's Law Dictionary* since 2011, and many entertaining examples are regularly published in *Above the Law*.[3]

Well, now comes a provocative new law review article on the topic – appropriately entitled "*Benchslaps*".[4] The article, by Prof. Joseph P. Mastrosimone of Washburn University School of Law, is a shot across the bow of the judiciary, arguing that judges who issue abusive benchslaps are engaging in clearly improper and unethical conduct.

Professor Mastrosimone starts his article with a heavy and repeated emphasis on the word "bully" — he even dedicates the piece, poignantly, "to all those who suffered under the thumb of a schoolyard or workplace bully." Judges who issue benchslaps, he argues, are simply big bullies in black robes, and the bench and bar should not abide such injudicious behavior. The very recent draft article posted on SSRN has already been noted and commented on by various legal publications and ethics blogs, including one review that finds the analysis of the article somewhat flawed.[5]

Certain federal appellate judges seem to be the source of the most withering benchslaps, most notably Judge Richard Posner of the Seventh U.S. Circuit Court of Appeals, and Judge Alex Kozinski of the Ninth Circuit.

Perhaps the granddaddy of all benchslaps was an opinion by Judge Posner comparing one unfortunate appellate counsel to an ostrich — including full color photographs of an ostrich, and a lawyer, sticking their heads in the sand, to illustrate the point that lawyers cannot simply ignore binding precedents. "The ostrich is a noble animal, but not a proper model for an appellate advocate." [6] That opinion received the award for the Best Flying Benchslap of 2012. [7]

And in a very recent decision, Judge Kozinski wrote that counsel in the case before him, Mr. Mitts, had demonstrated "obstinate incompetence" and had been "grossly negligent". The abuse goes on and on, ending with an innocent "I'm just trying to protect the public" flair: [8]

> "Potential clients, who will put their lives in Mitts' hands, as Brooks did, are entitled to know that this lawyer ignores client inquiries, misses jurisdictional deadlines and does not own up to his mistakes."

Kozinski said he is unaware of any disciplinary action against Mitts, and the State Bar of California may not be aware of his behavior. "Perhaps now it will be," Kozinski wrote.

One wonders whether a simple bar complaint from chambers might have been preferable to such a vicious personal attack on the attorney in a published appellate opinion. One wonders whether such judges even think about such restraint.

Are benchslaps a serious problem in Minnesota courts? Perhaps not. Those who know indicate that the judicial selection process screens candidates for potential demeanor issues, and part of basic judicial training in this state includes an emphasis on judicial demeanor, on not getting involved emotionally in the matter before the court – all things that should help deter any benchslap abuse. Nonetheless, a search of the phrase "benchslap" does pull up a handful of articles both in this paper and in *Minnesota Litigator.*

Cyber Threats – A new Ethics Issue and the Next Big Exposure for Law Firms

The Panama Papers story that broke last month illustrates the very real problem law firms face for failing to have secure systems for protecting client confidences. Hackers breached the systems of Panama-based law firm Mossack Fonseca and leaked a huge amount of data detailing how firm clients — politicians, businessmen and other public figures from across the world — used offshore companies to hide their income and avoid paying taxes.

Aside from the disastrous embarrassment and the ghastly PR problems this would create for any law firm, there is an increasingly serious ethics issue lurking here. Last year Rule 1.6 was amended by adding a new section (c) requiring that "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The Comments to the new Rule suggest that the ethical standard may well require much more than some law firms are currently doing. [9] Watch for it – someday, some local lawyer will be publicly reprimanded as a result of a computer hack/data breach at his or her firm.

In addition, law firms face incredible legal malpractice and other damage exposure in the event their client files are hacked. When the Panama Papers story broke, I wrote the following for *Security* Week, an industry news site: [10]

'Cyber Liability' has been a cutting-edge exposure issue for lawyers and law firms for a couple years now. Groups like the IADC and the American Bar Association have repeatedly featured this issue in their national conferences recently.

The Panama Papers story focuses the cyber issue on a law firm in a way few prior stories have done. A very recent article in the Times of London indicated that the law firm involved — Mossack Fonseca — had significant computer security failings that allowed hackers to infiltrate its systems and steal millions

of documents, quoting security experts who said the firm used outdated software containing security holes and failed to encrypt its emails. One expert noted that the firm's Outlook email system apparently hadn't been updated since 2009.

Any potential legal malpractice claim arising out of a law firm hack like this would focus on whether the firm was negligent in its security precautions. The standard of care that firms must meet evolves over time, but the fact that sub-standard procedures have already been identified in this case does not bode well for the firm.

Another issue is who could sue, and for what damage. I don't think you're going to see lawsuits claiming that the law firm's negligence damaged a client's goal of illegally evading taxes. Legal malpractice law generally does not allow claims against lawyers by clients engaged in criminal or fraudulent activity.

In addition to considering and implementing concrete steps to protect client information, law firms would be well advised to consider whether they are adequately insured against the substantial damage exposure and cost of a data breach.

Responding to this problem, the ABA Standing Committee on Lawyers Professional Liability has just published a very handy guide to insuring against this exposure, "Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy"[11] This 32-page paperback book, retailing for $19.95, has been described as "extremely useful for law firms that are looking to purchase a cyber liability policy" and "a must read for any law firm that recognizes that it's not a matter of 'if' but 'when' a data breach happens; (and) how a cyber policy can protect the firm and effectively manage the breach."

Chuck Lundberg is recognized nationally as a leader in the areas of legal ethics and malpractice. He served for twelve years on the Minnesota Lawyers Board, including six years as Board Chair. He retired last fall from Bassford Remele after 35 years of practice, and now advises attorneys and law firms through Lundberg Legal Ethics.

[1] A number of web sites are referred to throughout this article. In order to avoid interrupting the flow of the printed page for the readers of the paper version, they are placed in endnotes here.

[2] Needham, Six Benchslaps to Brighten Your Day, Lawyerist.com (10/2/15)

[3] Above the Law – which invented the term "benchslap" — publishes hilarious and cringe-worthy benchslaps from across the country almost every week. Here are a couple from just the past month or two: Lawyer Writes Stupid Brief, Fifth Circuit Lets Him Know ("Honestly, this isn't so much a benchslap as a targeted killing"); That Awkward Moment Where The Judge Marks Up Your Proposed Order To Say You're Misstating The Record; Federal Judge Prepared To Issue Benchslap After Getting Duped By Disbarred Rainmaker's Shenanigans ("This judge is pretty pissed"). ATL even has its own search page: http://abovethelaw.com/benchslaps/

[4] Benchslaps (scheduled for publication in the Utah Law Review).

[5] "A word about B**chslaps", Faughnan on Ethics (4/5/16) criticizes both the analysis of the article and its proposed corrective actions.

[6] See also Judges' Bullying Seen As Fuel For Bad Atty Behavior, Law360, and "Benchslaps and Judicial Ethics" in Legal Skills Prof Blog.

[7] Benchslaps and Judicial Ethics

[8] http://joshblackman.com/blog/2011/11/23/maybe-judge-posner-should-move-to-writing-illustrated-books/

http://joshblackman.com/blog/2012/12/18/the-8-best-benchslaps-of-2012/

http://www.abajournal.com/mobile/article/lawyer_who_filed_late_appeal_showed_obstinate_incompetence_kozinski_says?utm_content=buffer68541

http://abovethelaw.com/2016/03/angry-federal-appellate-judge-rips-criminal-defense-attorney-to-shreds/

[9] The Comment clearly places the burden on the lawyer to show "reasonable efforts" to avoid/deter hackers – ask yourself whether your firm can satisfy this standard now:

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation . . . if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

[10] http://www.securityweek.com/industry-reactions-panama-papers-feedback-friday

[11] See "ABA offers lawyers guide to evaluate, obtain cyber-liability insurance coverage"